

1 This listing of claims will replace all prior versions, and listings, of claims  
2 in the application:

3  
4 **Listing of Claims**

5  
6 Claim 1 (Original): A method comprising:

7 minting a stick of electronic assets by digitally signing with an issuer's  
8 signature a composite of user-provided data items including a user identity, a  
9 bottom asset from a bottom of the stick, and a length of the stick;

10 spending one or more assets from the stick at one or more vendors, wherein  
11 each expenditure with a particular vendor involves digitally signing with a user's  
12 signature a first asset from the stick to be spent and passing the user-signed first  
13 asset along with the issuer-signed composite to the particular vendor for  
14 verification and subsequently passing any additional assets to be spent without user  
15 signature to the particular vendor; and

16 depositing one or more assets collected by the particular vendor by digitally  
17 signing with the particular vendor's signature a composite of data items including  
18 the user-signed first asset and a last asset spent by the user from the stick and  
19 passing the vendor-signed composite along with the issuer-signed composite to the  
20 issuer.

21  
22 Claim 2 (Original): A method as recited in claim 1, further comprising  
23 storing the stick of electronic assets in a tamper-resistant electronic wallet.  
24  
25

1 Claim 3 (Original): A method as recited in claim 1, further comprising  
2 storing the stick of electronic assets in an electronic wallet constructed with a  
3 secure-processor architecture.

4  
5 Claim 4 (Original): A method as recited in claim 1, wherein the minting  
6 comprises minting the stick of assets using a blind signature protocol.

7  
8 Claim 5 (Original): A method as recited in claim 1, wherein the spending  
9 comprises:

10 concatenating a vendor identity with the first asset from the stick to form a  
11 payment request;

12 signing the payment request with a signature of the user;

13 submitting the user-signed payment request along with the issuer-signed  
14 withdrawal request to the vendor;

15 accepting the first asset as payment in an event that the user and the issuer  
16 are verified; and

17 subsequently passing any additional assets from the stick as payment to the  
18 vendor without digitally signing them with the user's signature;

19  
20 Claim 6 (Original): A method comprising:

21 minting a stick of electronic assets by digitally signing with an issuer's  
22 signature a composite of user-provided data items including a user identity, a  
23 bottom asset from a bottom of the stick, and a length of the stick;

24 spending one or more assets from the stick at one or more vendors, wherein  
25 each expenditure with a particular vendor involves digitally signing with a user's

1 signature a first asset from the stick to be spent and passing the user-signed first  
2 asset along with the issuer-signed composite to the particular vendor for  
3 verification and subsequently passing any additional assets to be spent without user  
4 signature to the particular vendor; and

5 depositing one or more assets collected by the particular vendor by digitally  
6 signing with the particular vendor's signature a composite of data items including  
7 the user-signed first asset and a last asset spent by the user from the stick and  
8 passing the vendor-signed composite along with the issuer-signed composite to the  
9 issuer, wherein the depositing comprises:

10 concatenating the user-signed first asset  $S_U(C_j)$ , a last asset spent from the  
11 stick  $C_k$ , and a run length  $RL$  of assets beginning with the first asset  $C_j$  and ending  
12 with the last asset  $C_k$  to form a deposit request;

13 signing the deposit request with a signature of the vendor:

$$S_V(S_U(C_j), C_k, RL)$$

14  
15  
16  
17 submitting the vendor-signed deposit request along with the issuer-signed  
18 withdrawal request to the issuer; and

19 crediting a vendor account with the run of assets in an event that the user,  
20 the vendor, the run, and the issuer are positively verified.

21  
22 Claim 7 (Original): A method as recited in claim 1, further comprising  
23 auditing the assets deposited by the vendor.  
24  
25

1 Claim 8 (Original): A method as recited in claim 1, further comprising  
2 auditing a sample of the assets paid by the user to the vendor.

3  
4 Claim 9 (Original): A method as recited in claim 1, further comprising  
5 selecting, at the vendor, a subset of less than all of the assets paid by the user to the  
6 vendor and submitting the subset of assets to an auditor for fraud evaluation.

7  
8 Claim 10 (Original): Distributed computer-readable media resident at the  
9 issuer, user, and vendor having computer-executable instructions to perform the  
10 method as recited in claim 1.

11  
12 Claim 11 (Original): Computers resident at the issuer, user, and vendor that  
13 are programmed to perform the method as recited in claim 1.

14  
15 Claim 12 (Original): A method for issuing electronic assets, comprising:  
16 forming a stick of  $L$  electronic assets  $C_i$  (for  $i=1, \dots, L$ ) where each asset  
17 can be derived from a preceding asset in the stick;  
18 signing the stick with a signature of a party issuing the assets;  
19 spending a first run of one or more assets from the stick at a first vendor;  
20 and  
21 spending a second run of one or more assets from the stick at a second  
22 vendor.

23

24

25

1 Claim 13 (Original): A method as recited in claim 12, further comprising  
2 storing the stick of electronic assets in a tamper-resistant electronic wallet.  
3

4 Claim 14 (Original): A method as recited in claim 12, further comprising  
5 storing the stick of electronic assets in an electronic wallet constructed with a  
6 secure-processor architecture.  
7

8 Claim 15 (Original): A method as recited in claim 12, wherein the forming  
9 comprises anonymously issuing the stick of assets using a blind signature protocol.  
10

11 Claim 16 (Original): A method as recited in claim 12, wherein the forming  
12 comprises:  
13

14 creating the stick of  $L$  electronic assets by computing:  
15

$$C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

16

17 where  $h(x)$  is a one-way hashing function of a value  $x$ .  
18

19 Claim 17 (previously amended): A method for issuing electronic assets,  
20 comprising:  
21

22 forming a stick of  $L$  electronic assets  $C_i$  (for  $i=1, \dots, L$ ) where each asset  
23 can be derived from a preceding asset in the stick; wherein the forming comprises:  
24

25 creating the stick of  $L$  electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

where  $h(x)$  is a one-way hashing function of a value  $x$ ;

constructing a withdrawal request having a user identity  $U$ , a user secret  $K$ , a last asset value  $C_L$  taken from a bottom of the stick, a denomination  $d$  indicating a value for the assets in the stick, an expiration  $t$ , and the value  $L$ ; and

signing the withdrawal request with a signature of an issuer:

$$S_H(U, K, d, C_L, t, L);$$

signing the stick with a signature of a party issuing the assets;

spending a first run of one or more assets from the stick at a first vendor;

and

spending a second run of one or more assets from the stick at a second vendor.

Claim 18 (Original): A method as recited in claim 12, wherein the spending comprises:

signing a first asset from the stick with a signature of the user:

submitting the user-signed asset along with the signed stick to the first vendor; and

in an event the first asset is accepted, subsequently submitting any additional assets from the stick without digitally signing them.

1 Claim 19 (Original): A method as recited in claim 12, further comprising  
2 auditing the assets from the first and second runs of assets for fraud.

3  
4 Claim 20 (Original): A method as recited in claim 12, further comprising  
5 auditing a sample of assets from the first and second runs of assets for fraud.

6  
7 Claim 21 (Original): A method as recited in claim 12, further comprising  
8 depositing the first and second runs of assets.

9  
10 Claim 22 (Original): Computer-readable media resident at the issuer and the  
11 user having computer-executable instructions to perform the method as recited in  
12 claim 12.

13  
14 Claim 23 (Original): Computers resident at the issuer and the user that are  
15 programmed to perform the method as recited in claim 12.

16  
17 Claim 24 (Original): A method for issuing electronic assets, comprising:  
18 creating, at a user, a stick of  $L$  electronic assets by computing:

19  
20 
$$C_i = h^i(x) \text{ (for } i=1, \dots, L)$$

21  
22 where  $h(x)$  is a hashing function of a value  $x$ ;

23 submitting a withdrawal request from the user to an issuer, the withdrawal  
24 request having a user identity  $U$ , a last asset value  $C_L$  taken from a bottom of the  
25 stick, and the value  $L$ , while omitting any vendor identity;

1 signing, at the issuer, the withdrawal request; and  
2 returning the signed withdrawal request to the user.  
3

4 Claim 25 (Original): A method as recited in claim 24, further comprising  
5 storing the stick of electronic assets and signed withdrawal request in a tamper-  
6 resistant electronic wallet.  
7

8 Claim 26 (Original): A method as recited in claim 24, further comprising  
9 storing the stick of electronic assets and signed withdrawal request in an electronic  
10 wallet constructed with a secure-processor architecture.  
11

12 Claim 27 (Original): A method as recited in claim 24, wherein the  
13 withdrawal request further has a user secret  $K$ , a denomination  $d$  indicating a value  
14 for the assets in the stick, and an expiration  $t$ .  
15

16 Claim 28 (Original): A computer-readable medium having computer-  
17 executable instructions that direct an electronic wallet to perform the method as  
18 recited in claim 24.  
19

20 Claim 29 (Original): A computer programmed to perform the method as  
21 recited in claim 24.  
22

23 Claim 30 (Canceled)  
24  
25



1 Claim 31 (Original): A method comprising:

2 creating, at a user, a stick of  $L$  electronic assets by computing:

3  
4 
$$C_i = h^i(x) \text{ (for } i=1, \dots, L)$$

5  
6 where  $h(x)$  is a hashing function of a value  $x$ ;

7 submitting a withdrawal request from the user to an issuer, the withdrawal  
8 request having a user identity  $U$ , a user secret  $K$ , a last asset value  $C_L$  taken from a  
9 bottom of the stick, a denomination  $d$  indicating a value for the assets in the stick,  
10 an expiration  $t$ , and the value  $L$ ;

11 signing, at the issuer, the withdrawal request:

12  
13 
$$S_I(U, K, d, C_L, t, L)$$

14  
15 returning the issuer-signed withdrawal request to the user;

16 initiating payment of one or more assets from the stick to a vendor having  
17 an identity  $V$ ;

18 concatenating, at the user, the vendor identity with a first asset  $C_j$  to be  
19 spent from the stick to form a payment request, and a depth  $D$  indicating a distance  
20 of the first asset from the bottom of the stick;

21 signing the payment request with a signature of the user:

22  
23 
$$S_U(C_j, D, V)$$

1 submitting the user-signed payment request along with the issuer-signed  
2 withdrawal request to the vendor;

3 accepting the first asset as payment at the vendor in an event that the user  
4 and the issuer are verified;

5 subsequently passing any additional assets from the stick as payment to the  
6 vendor without digitally signing them with the user's signature;

7 concatenating, at the vendor, the user-signed first asset, a last asset spent  
8 from the stick  $C_k$ , and a run length  $RL$  of assets beginning with the first asset  $C_j$   
9 and ending with the last asset  $C_k$  to form a deposit request;

10 signing the deposit request with a signature of the vendor:

$$S_v(S_u(C_j), C_k, RL)$$

14 submitting the vendor-signed deposit request along with the issuer-signed  
15 withdrawal request to the issuer; and

16 crediting a vendor account with the run of assets in an event that the user,  
17 the vendor, and the issuer are verified.

18  
19 Claim 32 (Original): A method as recited in claim 31, further comprising  
20 randomly selecting an asset from the assets paid by the user to the vendor and  
21 submitting the selected asset for audit.

22  
23 Claim 33 (Original): A method as recited in claim 31, further comprising  
24 auditing the assets deposited by the vendor with the issuer.  
25

1 Claim 34 (Original): A method for anonymously issuing electronic assets,  
2 comprising:

3 creating, at a user, a stick of  $L$  electronic assets by computing:

$$4 \quad C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

6 where  $h(x)$  is a hashing function of a value  $x$ ;

8 blinding the stick using a random value  $p$ , where:

$$10 \quad \text{Blind Stick} = p^e C_L \text{ mod } N$$

12 where  $C_L$  is a bottom asset on the stick;

13 submitting a withdrawal request from the user to an issuer, the withdrawal  
14 request having the blind stick and the value  $L$ ;

15 signing, at the issuer, the withdrawal request by computing:

$$17 \quad c = (p^e C_L)^{1/f} = p^L C_L^{1/f} \text{ mod } N$$

19 where  $e$  and  $f$  are public and private variables known by the issuer and  $e$  is  
20 known to everyone;

21 returning the signed withdrawal request to the user;

22 deriving a new bottom asset by computing:

$$24 \quad C_L^{1/f} = c/p^L \text{ mod } N.$$

1 Claim 35 (Original): A method as recited in claim 34, further comprising  
2 storing the blind stick of electronic assets and signed withdrawal request in a  
3 tamper-resistant electronic wallet.

4  
5 Claim 36 (Original): A method as recited in claim 34, further comprising  
6 verifying the bottom asset by computing  $C_L^{Lf}$  independently and comparing a result  
7 to the new bottom asset derived in said deriving ( $C_L^{Lf}$ )

8  
9 Claim 37 (Original): A method as recited in claim 34, further comprising  
10 storing the blind stick of electronic assets and signed withdrawal request in an  
11 electronic wallet constructed with a secure-processor architecture.

12  
13 Claim 38 (Original): A method as recited in claim 34, further comprising  
14 spending an asset from the blind stick by first sending the new bottom to a vendor  
15 for verification.

16  
17 Claim 39 (Original): A computer-readable medium having computer-  
18 executable instructions that direct an electronic wallet to perform the method as  
19 recited in claim 34.

20  
21 Claim 40 (Original): A computer programmed to perform the method as  
22 recited in claim 34.

23  
24 Claim 41 (Canceled)

1 Claims 42-50 (Withdrawn)

2  
3 Claim 51 (Original): An electronic asset system comprising:

4 an issuer wallet having a processor and storage, the issuer wallet digitally  
5 signing with an issuer's signature a composite of user-provided data items  
6 including a user identity, a bottom asset from a bottom of a stick of electronic  
7 assets, and a length of the stick;

8 a user wallet having a processor and storage to store the stick of electronic  
9 assets and issuer-signed composite and to spend one or more assets from the stick  
10 at one or more vendors, the user wallet spending one or more assets by digitally  
11 signing with a user's signature a first asset from the stick to be spent and passing  
12 the user-signed first asset along with the issuer-signed composite to the vendor for  
13 verification; whereupon verification, the user wallet subsequently passes any  
14 additional assets to be spent without user signature to the vendor; and

15 a vendor wallet having a processor and storage to store one or more assets  
16 spent by the user wallet, the vendor wallet depositing the assets collected from the  
17 user wallet by digitally signing with the particular vendor's signature a composite  
18 of data items including the user-signed first asset and a last asset passed in the  
19 stick received from the user wallet and passing the vendor-signed composite along  
20 with the issuer-signed composite to the issuer wallet for verification.

21  
22 Claim 52 (Original): An electronic asset system as recited in claim 51,  
23 wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-  
24 resistant.

1 Claim 53 (Original): An electronic asset system as recited in claim 51,  
2 wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-  
3 resistant constructed with a secure-processor architecture.

4  
5 Claim 54 (Original): An electronic asset system as recited in claim 51,  
6 wherein the issuer wallet signs the composite using a blind signature protocol.

7  
8 Claim 55 (Original): An electronic asset system as recited in claim 51,  
9 further comprising an auditing system to audit the electronic assets to detect  
10 whether assets have been used in a fraudulent manner.

11  
12 Claim 56 (Original): An electronic asset system as recited in claim 51,  
13 further comprising a probabilistic auditing system to sample a subset of less than  
14 all electronic assets to detect whether assets have been used in a fraudulent  
15 manner.

16  
17 Claim 57 (Original): An electronic wallet having memory and a processor,  
18 the electronic wallet being programmed to:

19 create a stick of  $L$  electronic assets by computing:

20  
21 
$$C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

22  
23 where  $h(x)$  is a hashing function of a value  $x$ ;

1 form a withdrawal request having a user identity  $U$ , a last asset value  $C_L$   
2 taken from a bottom of the stick, and the value  $L$ , while omitting any vendor  
3 identity;

4 submit withdrawal request to an issuer and receive the withdrawal request  
5 back with an issuer signature; and

6 store the signed withdrawal request and the stick.

7  
8 Claim 58 (Original): An electronic wallet having memory and a processor,  
9 the electronic wallet being programmed to:

10 create a stick of  $L$  electronic assets by computing:

$$C_i = h^i(x) \text{ (for } i=1, \dots, L)$$

11  
12 where  $h(x)$  is a hashing function of a value  $x$ ;

13  
14 form a withdrawal request having a user identity  $U$ , a last asset value  $C_L$   
15 taken from a bottom of the stick, and the value  $L$ , while omitting any vendor  
16 identity;

17  
18 submit withdrawal request to an issuer and receive the withdrawal request  
19 back with an issuer signature;

20 store the signed withdrawal request and the stick;

21 form a payment request for payment of one or more assets from the stick to  
22 a vendor having an identity  $V$ , the payment request having the vendor identity  $V$   
23 and a first asset  $C_j$  to be spent from the stick;

24 sign the payment request:

25

1  $S_U(C_j, V1)$ ; and

2  
3 submit the signed payment request along with the signed withdrawal  
4 request to the vendor.

5  
6 Claims 59-60 (Canceled).